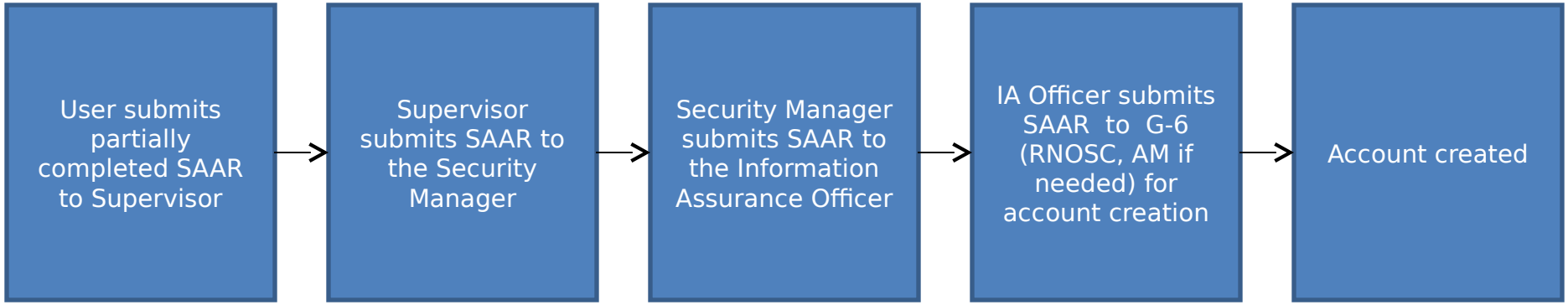
Procedures to Properly Complete A System Authorization Access Request (SAAR)


User submits partially completed SAAR to Supervisor
Supervisor submits SAAR to the Security Manager
Security Manager submits SAAR to the Information Assurance Officer
IA Officer submits SAAR to G-6 (RNOSC, AM if needed) for account creation
Account created

User fills out and submits partially completed SAAR to Supervisor

First step (USER)

- A partially completed SAAR consists of blocks 1 – 13 completely filled out.
- Use the directions included with the SAAR to fill out your portion.
- If you do not currently have access to a computer to complete training requirements or electronically fill out your SAAR, speak with your ISC.
- The system name options are (as needed):
  - On a SAAR for Classified access: MCW (SIPRNET); AMHS (SIPR); Sharepoint (SIPR).
  - On a SAAR for Unclassified access: NMCI (NIPRNET); AMHS (NIPR); MARFORRES domain; KCMA domain; CDC; MFR/PAO/MOBCOM Websites.
- Notate more specific application access needed in block 13.

User fills out and submits partially completed SAAR to Supervisor

First step (USER) (Continued)

- The location is where ever the user will reside the majority of the time while utilizing the account.
- The last two pages are the User Agreement. Review the agreement and initial where it says User Initials.
- **User's current PII Certificate & IA Certificate must accompany their SAAR for the accounts to be created.**
- User fills out and submits their partially completed SAAR to their supervisor. The supervisor is the person that signs in block 17. The user should digitally sign their SAAR (**Utilizing the U.S. Government ID Certificate NOT the e-mail certificate)** and send it via an encrypted email to their supervisor.

Supervisor submits SAAR to the Information Assurance Officer

Second Step (SUPERVISOR)

- Supervisors: ensure that blocks 1 – 13 are completely filled out and are accurate. If there is a problem notify the user and have them make the necessary corrections.
- Ensure that all required systems are correctly notated and all specific applications needed are listed in block 13, particularly if access is needed to: Right Now, PWST, Muster, or Contact and Screening.
- Once all information is correct please make the necessary additions to blocks 14 – 20b.
- Block 14 – You first must determine the type of access required. Authorized means the user will only receive normal access. Privileged means the user will receive extra privileges to make system changes.
- If Privileged access is required, list both the type of access required, the platform, system, or application it is required for, and the justification in Block 13.

Supervisor submits SAAR to the Information Assurance Officer

Second Step (SUPERVISOR) (continued)

- Block 15 – User requires access to: UNCLASSIFIED, CLASSIFIED or Other. When applying for a user account on the UNCLASSIFIED (NIPR) network select UNCLASSIFIED. When applying for a user account on the CLASSIFIED (SIPR) select CLASSIFIED. If neither fit the proper access please select other and correctly fill out the blank with the correct network.
- Block 16a – Access expiration date is the date the military user will execute a permanent change of station (PCS) or their End of Active Service (EAS). If the user is a contractor please use the company name, contract number and the contract expiration date.
- The SAAR must be forwarded by the supervisor to the Security Manager to fill out blocks 28 – 31 (OMB_MFR_SECURITY@usmc.mil) or (OMB MFR Security) in GAL.

Supervisor submits SAAR to the Information Assurance Officer

Third Step (Security Manager)

- The Security Manager complete Part III of the SAAR (blocks 28-32) and will then forward the SAAR on to the Information Assurance Officer.
- Once the action is completed please review the SAAR and then digitally sign the SAAR (**Utilizing the U.S. Government ID Certificate NOT the e-mail certificate)** and send it via an encrypted email to the Information Assurance Officer, this is the person that signs block 22 (marforres_g6_ia.fct@usmc.mil) or (MARFORRES G6 IA) in the GAL.

Information Assurance Officer submits SAAR back to User

Fourth Step (IA Office)

- The Information Assurance Officer will then receive and review the SAAR and will ensure the document has blocks 1 – 20b filled out completely and accurately. If problems exist IA will send the document back to the user with an explanation of the corrections needed.
- The Information Assurance Officer will not sign your SAAR until blocks 1 – 20b are filled out completely.
- The Information Assurance Officer will digitally sign the SAAR (**Utilizing the U.S. Government ID Certificate NOT the e-mail certificate)** and send it via an encrypted email to the RNOSC at: MFR_G6_RNOSC@usmc.mil.

User submits SAAR to G-6 for account creation

Fifth Step (Information Owner)

- The MFR G-6 personnel will review the completed SAAR and create the account. The user will be notified via email of their username and default password (if unclassified), also the G-6 personnel will send a copy of the completed SAAR to the user and will file a soft copy of the entire SAAR package.
- Some application's access will require additional time as they will need to be forwarded to G6 Application Management for follow on actions (MFR_APP_SERVICE_DESK@usmc.mil).
- In these instances (access to Right Now, PWST, Muster, or Contact and Screening) the Application Team will receive the SAAR, forward it on to the appropriate Application owner who will take necessary actions and forward the SAAR back to the user and CC MFR_G6_RNOSC@usmc.mil on the email with the completed SAAR.

This completes the presentation